MÓDULO

HERRAMIENTAS Y SEGURIDAD INFORMÁTICA PARA EL USO INSTITUCIONAL

SEGUNDO NIVEL DE DESARROLLO PROFESIONAL PARA EL PERSONAL DE NOMBRAMIENTO INSTITUCIONAL DEL ESCALAFÓN DE LOS SERVICIOS (NP2)

2026

SEMANA 3

UNIDAD 2:

MANUALES DE LA SEGURIDAD DE LA INFORMACIÓN DE CARABINEROS DE CHILE

1. MANUALES Y POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE CARABINEROS DE CHILE.

La Orden General Nro. 02786 de fecha 03 de agosto del año 2020 publicada en el Boletín Oficinal Nro. 4899, aprueba por parte de la Contraloría General de Carabineros, el **"Compendio de Manuales de Seguridad de la Información de Carabineros de Chile"**.

Actualmente son 13 los manuales de seguridad de la información de Carabineros de Chile".

Estos manuales finalidad establecer las obligaciones que le asisten a cada uno de los integrantes de la Institución, en el contexto de la normativa relacionada con el sistema de gestión de seguridad de la información, considerando y estableciendo a nivel Institucional la **"Política de Seguridad de la Información",** establecida y aprobada mediante Orden General Nro. 002930 de fecha 09 de junio del 2022.

Estos manuales regulan el sistema orientado a sentar las bases, para brindar protección a los activos de información de Carabineros de Chile. Además, se hace presente que consideran todo el marco normativo reglamentario necesario para el correcto desarrollo e implementación del referido sistema de seguridad de la información y ciberseguridad en Carabineros de Chile.

2. ¿QUÉ SON LOS ACTIVOS DE LA INFORMACIÓN?

En esta tercera Unidad, analizaremos diversos conceptos de la seguridad de la información. Comenzaremos analizando qué son los **Activos de la Información en Carabineros de Chile**.

- ✓ Los activos de la información, conforme a lo establecido en la Normativa ISO 27001, son todos los elementos que son relevantes durante la producción, procesamiento, emisión, almacenaje, comunicación, visualización y recuperación de la información que tenga un determinado valor para una organización o empresa.[1]

- ✓ La información es un bien que tiene un gran valor para la Institución, por lo tanto, esta debe ser protegida en forma apropiada con el fin de dar seguridad a la continuidad operacional, y con ello lograr minimizar algún daño que pueda ocasionar a la Institución, y así poder lograr extender la eficiencia y oportunidades de mejora de la gestión, en virtud de la Seguridad de la Información y Ciberseguridad.

[1] https://www.ioe-emp.org/es/organizaciones-internacionales/organizacion-internacional-para-la-normalizacion#:~:text=Qu%C3%A9%20es%20la%20ISO,normas%20internacionales%20y%20documentos%20relacionados.

✓ Además, se establece que un Activo de Información, es un "conocimiento o dato que tiene valor para la organización, por lo tanto, debe ser protegido". Es decir, todo aquello que tiene información y valor para Carabineros de Chile, y que, en consecuencia, debemos protegerlo e implementar diversas medidas acorde a su relevancia para lograr llevar a cabo diversas operaciones de la Institución, sin que pueda afectar la seguridad de la información.

En consecuencia, es importante lograr identificarlos, de manera de conocer los riesgos y controles necesarios de implementar para así garantizar su correcto uso y desempeño en Carabineros de Chile.

3. TIPOS DE ACTIVOS DE LA INFORMACIÓN

Como se mencionaba anteriormente, vamos a establecer que un activo, es aquel elemento que tiene algún valor para la organización y por lo que debe ser protegido. De manera que un activo de información contiene, trasmite y manipula información de la Institución.

La información de la organización, en Carabineros de Chile, es un activo, y actualmente, corresponde al más importante, por lo tanto, lo clasificaremos de la siguiente manera:

TANGIBLES:	**INTANGIBLES:**
•Son aquellos activos que disponen y contienen información, siendo fáciles de identificar, ya que estos se logran visualizar o identificar a simple vista, como lo son por ejemplo los computadores, servidores, disco duro, etc.	•Es aquel activo, que soporta la información dentro de un activo físico o material, y que son esenciales para una organización o Institución. •Un ejemplo claro, es un listado o nómina de funcionarios de Carabineros de Chile (*Información),* el cual esta alojado en una planilla Excel, que se encuentra alojada en un computador fiscal (Activo Material), en la oficina de partes de una alta repartición.

Es importante saber, al momento de mantener un registro o inventario de activos, que estos son la base para la gestión de los mismos, ya que tienen que incluir toda la información necesaria para mantenerlos operativos e identificados según su importancia, para poder resguardarlos.

Siempre, para un levantamiento del inventario de activos, debe contener varios parámetros, que nos permiten conocer la descripción de estos:

- Nombre del activo
- Descripción del activo
- Dependencia del activo
- Dueño del activo

Es por ello, que, dentro de la seguridad de la información, se articulan tres grandes dimensiones que siempre se deben garantizar, en virtud de que son los pilares necesarios para proteger la información, como lo son: Disponibilidad, Confidencialidad, Integridad, los cuales abordaremos en profundidad en la siguiente Unidad.

CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN

Activos de la Información

Base de datos

Correo electronico, libros, documentos electornicos.

Politicas o Manuales

Sistemas Operativos / Software

Activos Fisicos

Insfraestutura TI: edificios, Oficinas. DIRECCIÓN TIC

Hardware: Computador, Laptop, Disco Duro

Servidor Fisico

Equipos de mano; Alarma, entorno TI, Aire acondicionado

Activos Humanos

Empleados

Externos /Proveedores

Activos de Servicios

Cortafuego /Firewall

autenticación /http://autentificatic.carabineros.cl/

Servicios de Red

Es importante distinguir las diferentes categorías de los activos que puedan existir en su lugar o puesto de trabajo, por lo tanto, es conveniente clasificarlos conforme a lo siguiente:

DATOS:

Es toda aquella información, que se encuentra en cualquier formato, donde se logre generar, recoger, gestionar, trasmitir y destruir bases de datos o documentación, como por ejemplo: manuales, resoluciones exentas, políticas institucionales, normativas, planillas con datos, etc. Además, de una interpretación simbólica (numérica, algoritmo, alfabético, etc., de un determinado atributo o variable cualitativa o cuantitativa).

APLICACIONES:

Corresponde al software que se utiliza para la gestión de procesos, aplicaciones, sistemas operáticos, sistemas de detección de intrusos, sitios web y sus aplicaciones.

PERSONAL:

En esta categoría, encontramos a todo el personal que integra la planta de Carabineros de Chile, a los usuarios de diversas plataformas institucionales, clientes, proveedores, entre otros, y en general a todos aquellos que tengan acceso de una manera u otra a los activos de la información de la Institución.

INSTALACIONES;

Son los lugares físicos en los que se alojan los diversos activos de la información y sistemas informáticos, es decir hablamos de oficinas, edificios, data center, etc.

HARDWARE:

Se refiere a los equipos físicos necesarios para lograr desarrollar la labor diaria en Carabineros de chile: servidores, dispositivos móviles, cableadas, etc., en otras palabras, corresponde al equipo o soporte físico de la informática.

RED:

Se refiere a los dispositivos y/o equipos interconectados entre si a través de un medio, que intercambian datos e información y comparten diversos recursos. Por ejemplo: dispositivos de conectividad a redes como routers, switches.

MÓDULO

HERRAMIENTAS Y SEGURIDAD INFORMÁTICA PARA EL USO INSTITUCIONAL

SEGUNDO NIVEL DE DESARROLLO PROFESIONAL PARA EL PERSONAL DE NOMBRAMIENTO INSTITUCIONAL DEL ESCALAFÓN DE LOS SERVICIOS (NP2)

2026

SEMANA 4

4. ACTIVOS DE LA INFORMACIÓN EN CARABINEROS DE CHILE

Durante la presente Unidad, se ha definido el concepto, tipo y clasificación de los activos de la información, en una organización como Carabineros de Chile. Es importante conocer a nivel Institucional, con qué tipos de activos contamos y por qué es importante velar por el cuidado de estos. Respecto de la seguridad de la información y la ciberseguridad, y para evitar que ocurran incidentes que puedan afectar gravemente a la Institución, es que se detallan algunos ejemplos.

Es importante que durante su trayectoria institucional, en el lugar en el que se desempeñe, pueda aplicar conocimientos sobre el resguardo de la información, generando por ejemplo, un inventario de activos de la información, que no es más que una lista de recursos con información valiosa de su lugar de trabajo.

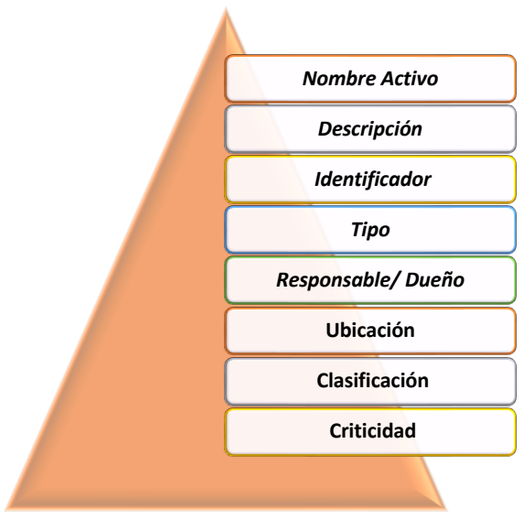
Nombre del activo
Servidores
Sitios Web
Software
Proveedores
Base de Datos
Correos Electrónicos
Soporte de información
Libros de servicios de Guardia
Hardware
Infraestructura
Red de telefonía
Recurso Humano
Plataforma Cisco Webex
Soporte Técnico
Archivos (Documentos Físicos y Digital)
Disipativos de Red
Oficinas
Cajas de Seguridad
Dispositivos de almacenamiento
Control de Acceso del personal – Proveedores
Otros Dispositivos de seguridad
Teletrabajo
Mensajería Instantánea
Estaciones de trabajo (Oficinas)
Servicio de Autenticación de Usuarios (Intranet)

5. USO CORRECTO DE LOS ACTIVOS DE LA INFORMACIÓN.

A raíz de anterior, es transcendental siempre considerar dar un uso correcto a los diferentes activos de la Información. Esto se logra recabando la mayor cantidad de antecedentes, por lo que es importante poder contar con las características del activo, ya que esto permitirá que dicho inventario nos ayude a contar con información suficiente para realizar proyectos de adquisición, o de mejoras, entre otros. Por otro lado, también puede utilizar esta información ante algún incidente

que lo pueda afectar y de esa manera poder reaccionar de manera oportuna ante posibles hechos que puedan involucrar el funcionamiento de estos.

Es por ello, que para el uso correcto de estos activos, se debe contar con un registro de aquellos que nos permita obtener información relevante de cada uno, por ejemplo:



http://www.dipres.gob.cl/598/articles-51683_intro_Guia_Metodologica04_2015.pdf

1.- Nombre Activo: Nombre de identificación al que pertenece (modelo, marca, etc.)

2.- Descripción: Descripción breve, de manera que sea claramente identificable por los usuarios y/o colaboradores.

3.- Identificador: Código único para el activo, que lo identifica (B.C.U).

4.- Tipo: Corresponde a establecer su naturaleza, y que permita ser identificado por sus usuarios, por lo tanto, se utilizan algunos valores como: software, base de datos, infraestructura física, recurso humano, sistema, servicios, entre otros.

5.- Responsable: Se refiere al funcionario encargado del activo, el cual tendrá la responsabilidad de su uso, cuidado y mantención.

6.- Ubicación: Debe detallarse de manera clara el lugar físico, la ubicación del activo de la información. Es decir, por ejemplo, saber en qué dependencias físicas se encuentra un Hardware o en su defecto si es algún sistema electrónico, digital o lugar virtual donde se encuentra, como sitios webs, páginas, sistemas institucionales o las diferentes plataformas que puede utilizar.

7.- Clasificación: Respecto a este punto, hace referencia a la protección que se le va a otorgar a la información de acuerdo, a su integridad, disponibilidad y confidencialidad.

8.- Criticidad: Este punto hace mención a poder establecer una priorización de los activos que fueron inventariados, es decir, nos permite obtener un valor general del activo, de acuerdo a su clasificación; por ejemplo; alta, media o baja.

Variables asociadas a la criticidad	Grado	Significado
CONFIDENCIALIDAD	Pública	El activo no tiene restricciones de acceso.
	Reservada	Activo de información cuyo acceso no autorizado tiene impacto para la institución o terceros.
INTEGRIDAD	Baja	Activo de Información cuya modificación no deseada tiene consecuencias con impacto leve para la institución o terceros.
	Media	Activo de Información cuya modificación no deseada tiene consecuencias con impacto significativo para la institución o terceros.
	Alta	Activo de Información cuya modificación no deseada tiene consecuencias con impacto grave para la institución o terceros
DISPONIBILIDAD	Baja	Activo de Información cuya inaccesibilidad, tiene impacto leve para la institución o terceros.
	Media	Activo de Información cuya inaccesibilidad, tiene impacto significativo para la institución o terceros.
	Alta	Activo de Información cuya inaccesibilidad, tiene impacto grave para la institución o terceros.

Tabla 1: Valores para Cálculo de Criticidad

http://www.dipres.gob.cl/598/articles-51683_intro_Guia_Metodologica04_2015.pdf

Por lo tanto, es importante que pueda identificar los diversos activos de información que existen en Carabineros de Chile, específicamente dentro del área en la que se desempaña profesionalmente, como por ejemplo, al trabajar con una base de datos que pueda crear y que es utilizada por la organización, a través de un medio digital o papel físico en diferentes áreas, la utilización de hardware y de software, que sin lugar a duda serán utilizados para el procesamiento o almacenamiento de información, es indispensable darles un buen uso, permitiendo con ello que los encargados de la seguridad de la información en la institución, puedan llevar a cabo una buena gestión del uso de los activos de información.

MÓDULO

HERRAMIENTAS Y SEGURIDAD INFORMÁTICA PARA EL USO INSTITUCIONAL

SEGUNDO NIVEL DE DESARROLLO PROFESIONAL PARA EL PERSONAL DE NOMBRAMIENTO INSTITUCIONAL DEL ESCALAFÓN DE LOS SERVICIOS (NP2)

2026

SEMANA 5

UNIDAD 3:

ROL INSTITUCIONAL SOBRE MATERIAS DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

La seguridad de la información y la ciberseguridad son dos factores primordiales, que las organizaciones y los usuarios debemos tener en cuenta cuando se accede tanto a activos físicos y/o lógicos, como también a la red en el ciberespacio.

La expansión de las nuevas tecnologías, a lo largo de estos últimos años, ha cambiado de forma notable debido a la incidencia de la tecnología. Hemos visto como se han ido transformando aspectos tan esenciales en nuestro mercado laboral, como la forma de acceder a la información, las posibilidades a la hora de compartir ideas y, sobre todo, nuestra manera de comunicarnos e interactuar con los otros, lo que nos ha permitido como institución, poder materializar diversos procesos académicos que son impartidos bajo la modalidad on line, es por ello, que se hace necesario que actualmente se adquieran conocimientos básicos sobre esta área.

Esta revolución digital, que actualmente vivimos como sociedad, nos ha abierto un mundo de oportunidades, pero este cambio viene acompañado de diversos peligros que pueden afectarnos como institución y como personas.

1. CONCEPTOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD.

¿QUÉ ES LA SEGURIDAD DE LA INFORMACIÓN?

La seguridad de la información, se define como un **conjunto de medidas preventivas y reactivas** de toda organización y de sus sistemas tecnológicos, permitiendo y haciendo posible proteger la información manteniendo la confidencialidad, disponibilidad e integridad.

Se refiera a la protección y resguardo de la información integral de personas, instituciones, organizaciones, gobiernos, empresas, entre otros, permitiendo proteger la información de todo tipo de riesgo, no importando si son digitales, físicas u otro medio, por ejemplo, un ataque informático, un incendio, terremoto u otra situación que pueda afectar a los activos.

Es importante, señalar que no se debe confundir el término "**Seguridad de la Información**" con el de "**Seguridad Informática**", ya que esta última se encarga de **proteger la integridad y privacidad de la información almacenada en un sistema informático de ciberdelincuentes**, ya que estos buscan siempre obtener ganancias o sustento económico de la información adquirida o acceder a ella.

Es importante precisar que la **Seguridad de la Información**, establece toda su base en los siguientes principios:

INTEGRIDAD:

Todo sistema que gestiona la información debe garantizar la integridad de la misma, es decir, **la información se muestra tal y como fue concebida, sin** alteración alguna o manipulación que no hayan sido autorizadas expresamente por alguien previamente autorizado.

Por lo tanto, su modificación no deseada trae consecuentes que pueden generan distintos niveles de impacto para una institución o terceros.

Ejemplo: En la plataforma de educación a distancia de este Centro Nacional, para cada uno de sus Niveles de desarrollo Profesional, los documentos son cargados bajo el formato PDF., y no pueden ser modificados ni alterados por ningún estudiante, es decir, la integridad de ese archivo o de otros cargados en plataforma solo pueden ser modificado por quienes estan autorizados.

DISPONIBILIDAD:

La característica de la disponibilidad es que garantiza que la información estará disponible en todo momento para las personas, empresas, y/o instituciones autorizadas para su manejo y conocimiento. Es decir, deben estar puestas a disposición de quienes necesiten acceder a ella.

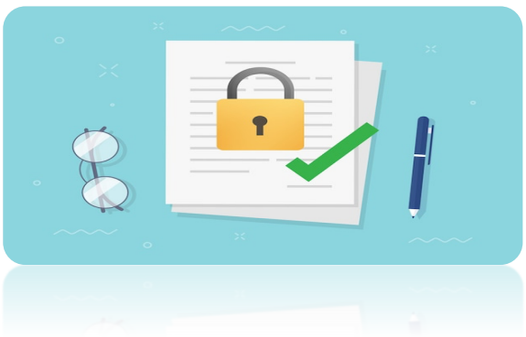
De manera simple, la característica que define la disponibilidad es que siempre sea accesible para un usuario, aplicación, sistema de computación, o página web, entre otros., cuando sea requerida.

Ejemplo: Siguiendo con el ejemplo anterior, el área encargada de la Seguridad Informática de este Centro de Perfeccionamiento debe mantener las plataformas de educación a distancia disponibles para la totalidad de alumnos y operativas las 24 horas del día, los 7 días de la semana, lo que les permitirá ingresar y obtener su material de estudio, y también rendir sus evaluaciones en las fechas establecidas, sin inconvenientes.

CONFIDENCIALIDAD:

Este término permite garantizar que solo las personas o instituciones autorizadas puedan tener acceso a la información y datos, por lo tanto, estos no podrán divulgarse sin su autorización o permiso. En consecuencia, debe comprender que este término está relacionado con mantener la información, las redes y sistemas seguros frente a un acceso que no esté autorizado.

Ejemplo: Uniéndome a los ejemplos anteriores, al descargar material de estudio o en su defecto cuando carguen un trabajo de aplicación de uno de los módulos, la confidencialidad permite que a ese documento no tengan acceso otras personas que no estén autorizadas para verlo.



OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

Busca que la totalidad de la información esté protegida, para garantizar que esté exenta de modificaciones de usuarios no autorizados.
INTEGRIDAD
DISPONIBILIDAD
INFORMACIÓN
CONFIDENCIALIDAD
Garantizar que la información se encuentre a disposición de quienes deben acceder a ella.
Prevenir la divulgación de información a personas no autorizados.

https://alonso7431.wordpress.com/2016/06/27/seguridad-informatica/

¿QUÉ ES LA CIBERSEGURIDAD?

Entendiendo que es la seguridad de la información, podemos señalar que la ciberseguridad cuenta con diferentes conceptos, los cuales se señalan a continuación:

- ✓ La capacidad de proteger o defender el uso del ciberespacio de ciberataques[2].

[2] https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

- ✓ Medidas y controles que garantizan la confidencialidad, integridad y disponibilidad de activos del sistema de información, incluido hardware, software, firmware e información que se procesa, almacena y comunica[3].

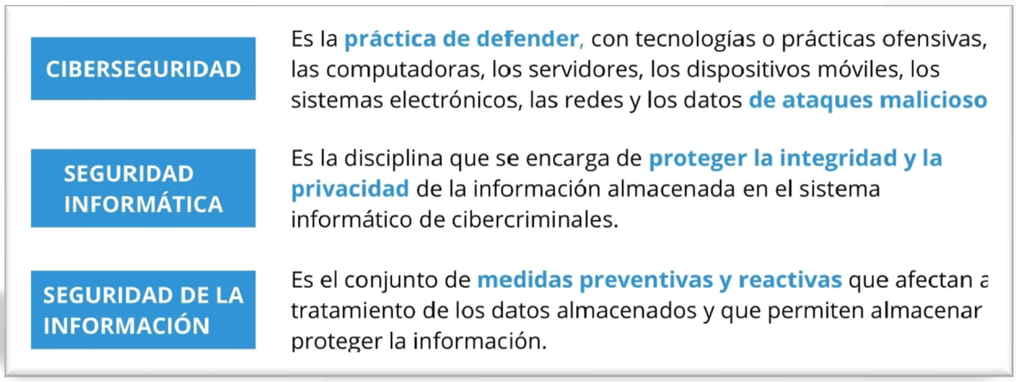
Cuando nos referimos a ciberseguridad, hablamos de un conjunto de soluciones o servicios que podemos implementar en una organización, empresa o en la Institución, para defendernos contra ataques cibernéticos. Por lo tanto, uno de los objetivos que podemos señalar, es que busca proteger la información que está dentro de los entornos digitales en los sistemas interconectados, considerado que la Ciberseguridad está inserta dentro de la seguridad de la información.

A raíz de lo anterior, la ciberseguridad es un esfuerzo continuo que busca proteger a las personas, organizaciones, instituciones públicas, privadas y de gobierno, de los ataques que hoy en día existen y se materializan a través de lo digital, mediante la protección de sus sistemas y datos en red central del uso o daño que no esté autorizado.

A continuación, se detalla que la ciberseguridad es parte componente de la seguridad de la información, y se entrega un breve un resumen que explica los términos vistos durante la presente Unidad.

SEGURIDAD DE LA INFORMACIÓN:
- Presenta Soluciones
- Mantiene la Confidencialidad, Disponibilidad e Integridad.
- Elementos a proteger: Recurso Humano, Equipos, Infraestructura y Hardware, Información Física y Digital.
- Seguridad Física, Operacional, Gestión.
-Establece Normas, Metodologías, Leyes, Protocolos.
erseguridad
ositivos
- Claves que utilizamos para iniciar o registrarnos en alguna ción o página web.
- Programa que detecta cualquier aza, como los virus, y la a de nuestro dispositivo.
- Software
- Ingeniería social

CIBERSEGURIDAD, SEGURIDAD INFORMÁTICA Y SEGURIDAD DE LA INFORMACIÓN


CIBERSEGURIDAD
Es la práctica de defender, con tecnologías o prácticas ofensivas, las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques malicioso
SEGURIDAD INFORMÁTICA
Es la disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en el sistema informático de cibercriminales.
SEGURIDAD DE LA INFORMACIÓN
Es el conjunto de medidas preventivas y reactivas que afectan a tratamiento de los datos almacenados y que permiten almacenar proteger la información.

https://www.lisainstitute.com/blogs/blog/diferencia-ciberseguridad-seguridad-informatica-seguridad-informacion

[3] https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=913810

2. CONCEPTOS Y TIPOS DE AMENAZAS DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD.

Como se ha explicado y detallado durante el presente módulo, nuestra sociedad va cambiando de una forma muy rápida debido a la incidencia de la tecnología. El impacto que existe sobre la nueva tendencia de la revolución digital, deriva del extraordinario progreso que tiene la tecnología, y que nos permite acceder de manera rápida y accesible a toda la información que pueda existir a través de internet, por cualquier medio o dispositivo tecnológico.

Es por ello, que se realizan diversas estrategias por parte de los encargados de velar por la seguridad de la información y ciberseguridad, para lograr contrarrestar las diversas amenazas que existen en el ciberespacio y poder encontrar y aplicar estrategias necesarias para combatirlas, evitando que pueda afectar a los diversos activos de la información, a través de amenazas o vulnerabilidades.

En este sentido, existen amenazas frecuentes y que se ven diariamente en los medios de comunicación y que afectan directamente a los usuarios que utilizan diversas plataformas digitales, como también gravemente a grandes empresas o pymes; muchas de estas últimas han tenido que cerrar, a raíz del robo de información del que han sido víctimas, ya que no han podido reponerse de sus efectos, y una vez que son atacadas, no cuentan con recursos para aplicar suficientes herramientas de seguridad.

A continuación, indicaremos cuáles son algunas de las principales amenazas de la seguridad informática y como se realizan los diferentes tipos de ciberataques, esto con la finalidad de hacer conciencia en los usuarios que utilizan diversos medios tantos físicos como lógicos, evitando ser víctima de estos delitos.

TIPOS DE MALWARE:

Malware es un término que abarca cualquier tipo de software malicioso diseñado para dañar o explotar cualquier dispositivo, servicio o red programable. Los delincuentes cibernéticos generalmente lo usan para extraer datos que pueden utilizar como chantaje hacia las víctimas para obtener ganancias financieras.

Dichos datos pueden variar desde datos financieros, hasta registros de atención médica, correos electrónicos personales y contraseñas. La variedad de información que puede verse comprometida se ha vuelto ilimitada.[4]

[4] https://www.mcafee.com/escl/antivirus/malware.html#:~:text=Malware%20es%20un%20t%C3%A9rmino%20que,v%C3%ADctimas%20para%20obtener%20ganancias%20financieras.

Spyware

Diseñado para rastrear y espiar. El software espía monitorea su actividad en línea y puede registrar cada tecla que presiona en el teclado, así como capturar casi todos sus datos, incluida información personal y confidencial, como sus datos bancarios en línea. El software espía lo hace modificando la configuración de seguridad de sus dispositivos.

El spyware con frecuencia se agrupa con el software legítimo o con caballos troyanos.

Ransomware

Este malware está diseñado para mantener cautivo un sistema computacional o los datos que contiene hasta que se realice un pago. El ransomware generalmente funciona cifrando sus datos para que no pueda acceder a ellos.

Algunas otras versiones de ransomware pueden aprovechar vulnerabilidades específicas del sistema para bloquearlo. El ransomware a menudo se propaga a través de correos electrónicos de phishing que lo alientan a descargar un archivo adjunto malicioso o a través de una vulnerabilidad.

Rootkit

Este malware está diseñado para modificar el sistema operativo para crear una puerta trasera, que los atacantes pueden usar para acceder a su computadora de forma remota. La mayoría de los rootkits aprovecha las vulnerabilidades de software para ganar acceso a recurso que normalmente no debería ser accesibles (escalada de privilegios) y modificar los archivos del sistema.

Los rootkits también pueden modificar las herramientas de monitoreo y análisis forense del sistema, lo que los hace muy difíciles de detectar. En la mayoría de los casos, un equipo infectado por un rootkit debe borrarse y reinstalarse cualquier software necesario.

Virus

Un virus es un tipo de programa informático que cuando se ejecuta, se replica y se adjunta a otros archivos ejecutables, como un documento, insertando su propio código. La mayoría de los virus requieren la interacción del usuario final para iniciar la activación y se pueden escribir para que actúen en una fecha u hora específica.

Los virus pueden ser relativamente inofensivos, como los que muestran una imagen divertida. O pueden ser destructivos, como los que modifican o eliminan datos.

Los virus también pueden programarse para mutar a fin de evitar la detección. La mayoría de los virus ahora se esparcen por unidades USB, discos ópticos, recursos de red compartidos o correo electrónico.

Ingeniería social

La ingeniería social es un conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales, infecten sus computadoras con malware o abran enlaces a sitios infectados

Scareware

Este es un tipo de malware que utiliza tácticas de «miedo» para engañarlo para que tome una acción específica. El scareware consiste principalmente en ventanas emergentes que aparecen para advertirle que su sistema está en riesgo y necesita ejecutar un programa específico para que vuelva a funcionar normalmente.

Si acepta ejecutar el programa específico, su sistema se infectará con malware.

Adware

El adware a menudo se instala con algunas versiones de software y está diseñado para entregar automáticamente anuncios a un usuario, la mayoría de las veces en un navegador web. ¡Lo sabes cuando lo ves! Es difícil ignorarlo cuando te enfrentas a anuncios emergentes constantes en tu pantalla.

Es común que el adware venga con spyware.

Rogues

Estos programas generan una gran cantidad de alarmas sobre virus informáticos en nuestro sistema. Posteriormente, te ofrecen la solución dándote la opción de descargar un antivirus que se instala en tu sistema. Una vez que los has descargado, realiza un chequeo tras el cual informa de la eliminación del peligroso virus que te amenazaba.

El método de estafa consiste en la proposición de la descarga del antivirus completo, que deberás pagar. El pago puede ser en páginas poco seguras donde se pueden hacer con tus datos. Evidentemente, el antivirus, su búsqueda y la eliminación de los virus no han sido reales, sino datos completamente falsos.

3 MEDIDAS DE SEGURIDAD BÁSICAS PARA ENFRENTAR AMENAZAS DE CIBERSEGURIDAD.

Es importante conocer algunas buenas prácticas aplicadas o medias de seguridad básicas, sobre el uso de la de tecnología e información institucional, por lo que se señalarán recomendaciones que debe considerar para estar siempre atento, y evitar ser víctimas de ciberdelincuentes.

1.- CONTROLES DE ACCESO FÍSICO:

En este punto nos estamos refiriendo a áreas restringidas, el ingreso de personal no autorizado siempre debe contar con una fiscalización adecuada.

Además, evitar la exposición de información sensible, que puede estar en nuestros escritorios, es decir, por ejemplo, no debemos dejar antecedentes importantes, tales como un posit con contraseñas, en el escritorio o pantalla del computador, entre otras. Este tipo de control que existe actualmente, es denominado “escritorio limpio”.

Siempre es recomendable, además, una buena destrucción de documentos oficiales, como por ejemplo, documentos secretos o reservados.

En una comisaria, por ejemplo, tenemos la sala de arma, donde se mantienen actas de entrega o recepción de armamento o munición, entre otros. Este es considerado un activo de la información muy importante para un posible delincuente, por lo tanto, se debe velar por su cuidado con la finalidad que no llegue a terceros.

2.- CORREO ELECTRÓNICO:

Lo ideal es poder utilizar el correo electrónico Institucional, en caso contrario y utilizar uno ajeno, es recomendable poder verificar las extensiones que vienen en archivo adjunto, antes de abrirlos. Por lo que, cualquier recomendación que nos llegue desde una red social, o un email con un link, puede convertirse en un factor de riesgo. Ante alguna duda, lo mejor es poder digitalizar la URL, que viene adjunta en nuestro navegador.

3.- CUIDADO BÁSICOS CON EL COMPUTADOR, NOTEBOOK:

Es recomendable la utilización de contraseñas propias y robustas, evitando por ejemplo dejarlas a la vista de terceras personas.

Evitar de todas maneras conectar dispositivos externos, como pendrive, disco duro, etc. desconocidos, sin autorización por parte de los encargados de la seguridad de la información.

Esto se fundamenta en que una persona malintencionada y que quiera obtener información o efectuar un ataque, puede dejar en alguna dependencia institucional, un pendrive o dispositivo externo, para que este sea utilizado y así poder obtener fraudulentamente antecedentes o simplemente para tratar de vulnerar nuestros dispositivos. Por lo que es importante siempre ser desconfiado.

4.- REDES INALÁMBRICAS Y NAVEGACIÓN WEB:

Es importante navegar en sitios seguros, con conexión segura. Es super tentador, conectarse a un servicio de Wife, por ejemplo, gratuito, pero esto puede permitir que personas o ciberdelincuentes estén monitoreando lo que estamos realizando, o que estamos revisando, o simplemente pueden vulnerar nuestra seguridad.

5.- MANEJO DE SITUACIONES SOSPECHOSAS:

Es importante que al momento de detectar alguna anomalía, que pueda afectar la seguridad de la información institucional, como, por ejemplo, si al abrir un correo sospecha que contenga algún tipo de malware, debe informar de inmediato a sus superiores, para escalar al área respectiva logrando con ello evitar que pueda afectar algún activo de la información.

6.- CONCIENTIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD:

Es muy importante que los encargados de dar cumplimiento a las Políticas de Seguridad de la Información, proporcionen diversas capacitaciones a los usuarios, en este caso a la totalidad de los funcionarios de carabineros de chile, con la finalidad de educar e indicar los procedimientos sobre seguridad de la información, ante algún hecho que los pueda afectar.

Es importante mencionar, que a pesar de los cuantiosos esfuerzos técnicos y de inversión en infraestructura para protegernos de los ataques cibernéticos, hoy en día las organizaciones, en general, enfrentan un desafío común, que es crear conciencia entre sus colaboradores acerca de la seguridad de la información.

A veces, creemos o pensamos que las mayores amenazas que afectan a la seguridad de la información provienen desde afuera, sin embargo, una gran proporción de los incidentes son ocasionados por empleados o usuarios desinformados, que simplemente no tienen conciencia real del alcance de sus acciones respecto a la Seguridad de la Información y Ciberseguridad.

NOTICIAS SOBRE SITUACIONES QUE HAN AFECTADO A ENTIDADES TANTO PUBLICAS COMO PRIVADAS.

Chile es el cuarto país de América Latina con más intentos de ciberataques por mensajes fraudulentos

Por Florencia Ortiz
Con información de Comunicado de Prensa.

Relacionados

- Hackean web del Sernac y Gobierno activa protocolo para frenar eventuales consecuencias
- Bases de datos de Sernac cumplieron 5 días secuestradas por hackers: sólo la web dio ciertos guiños
- CSIRT emite alerta de seguridad cibernética para todo el Estado tras hackeo a Sernac

Contenido | Pexels 1639 visitas

Chile es el cuarto país de América Latina que más recibe intentos de ataques de phishing (mensajes fraudulentos). Especialistas entregaron algunos consejos para que los usuarios estén mejor protegidos.

LITORALPRESS

Otra vez: Poder Judicial reporta nuevo virus que ahora estaría afectando a computadores con Windows 10

De acuerdo con información transmitida hasta ahora, serían tres los tribunales los afectados.

Leslie Ayala y Catalina Batarce **28 SEP 2022** 06:04 PM Tiempo de lectura: 1 minuto

Jueves 06 octubre de 2022 | 19:35

"No hacer click en ningún enlace": Entel informa que su cuenta de ayuda en Twitter fue vulnerada

Por Jean Valencia

LITORALPRE

Superintendente de Bancos: El hackeo a tarjetas de crédito es un "incidente grave"
#TUMAÑANA
FILTRAN DATOS DE 14 MIL TARJETAS DE CRÉDITO

MÁS DE 340 GIGAS DE INFORMACIÓN. CIPER MANTIENE EN RESERVA LOS DATOS QUE PUEDEN AFECTAR LA SEGURIDAD NACIONAL

Hackeo masivo al Estado Mayor Conjunto expuso miles de documentos de áreas sensibles de la defensa

SP Superintendencia de Pensiones
Gobierno de Chile
Estimado(a),
De acuerdo a sus instrucciones hemos iniciado la gestión de retiro del 10% de su cuenta de ahorros AFP hacia la cuenta terminada en 00411. En este correo podrá encontrar un documento adjunto con todos los detalles de la operación.
Este correo ha sido generado automáticamente por nuestro sistema o por solicitud del usuario.
Por favor no responda este correo.
Gracias Superintendencia de Pensiones.
FALSO
CSIRT

3.4 PROTECCIÓN DE DATOS PERSONALES EN EL ÁMBITO INSTITUCIONAL

La protección de los datos personales constituye un elemento fundamental dentro de la seguridad de la información, especialmente en instituciones públicas que manejan información sensible de la ciudadanía.

En Chile, el tratamiento de los datos personales se encuentra regulado por la Ley N° 21.719 sobre Protección de Datos Personales, normativa que establece principios y obligaciones para las instituciones respecto al uso, almacenamiento y protección de la información personal.

Se consideran datos personales toda información relativa a una persona natural identificada o identificable, tales como nombre, número de identificación, domicilio, teléfono, correo electrónico u otros registros asociados a una persona.

En el ejercicio de sus funciones, los funcionarios pueden tener acceso a información personal de ciudadanos o de otros integrantes de la institución, por lo que resulta fundamental resguardar dicha información y utilizarla únicamente para los fines institucionales correspondientes.

La correcta protección de los datos personales contribuye a prevenir accesos no autorizados, filtraciones de información y el uso indebido de datos, fortaleciendo la seguridad de la información y la confianza de la ciudadanía en las instituciones públicas.

V. BIBLIOGRAFÍA:

BIBLIOGRAFÍA OBLIGATORIA

- Carabineros de Chile (15 de octubre de 2019). Orden General 2694. “Manual de Organización de Seguridad de la Información de Carabineros de Chile. http://portalnormativo.carabineros.cl/buscadorportal/get_document/15071
- Carabineros de Chile (9 de junio de 2022). Orden General 2930. “Políticas de Seguridad la Información Carabineros Chile”. http://portalnormativo.carabineros.cl/buscadorportal/get_document/15707
- Ley N°21459 de 2022. “ESTABLECE NORMAS SOBRE DELITOS INFORMÁTICOS, DEROGA LA LEY N° 19.223 Y MODIFICA OTROS CUERPOS LEGALES CON EL OBJETO DE ADECUARLOS AL CONVENIO DE BUDAPEST”. 20 de junio 2022. https://www.bcn.cl/leychile/navegar?idNorma=1177743
- Carabineros de Chile (12 de noviembre de 2021). Orden General 2829. “Sistema de Documentación Electrónica”. http://portalnormativo.carabineros.cl/buscadorportal/get_document/15660
- Ley Nro. 19.799 de 2002. “sobre Documentos Electrónicos, firma electrónica y servicios de certificación de dicha firma y su reglamento” 25 de marzo de 2002. https://www.bcn.cl/leychile/navegar?idNorma=196640
- Ley Nro. 21719 (2024). “REGULA LA PROTECCIÓN Y EL TRATAMIENTO DE LOS DATOS PERSONALES Y CREA LA AGENCIA DE PROTECCIÓN DE DATOS PERSONALES”. 25 de noviembre de 2024 https://www.bcn.cl/leychile/navegar?idNorma=1209272
- Carabineros de Chile. (2000) Reglamento de documentación, N°22, de Carabineros de Chile. http://portalnormativo.carabineros.cl/buscadorportal/get_document/2150

BIBLIOGRAFÍA COMPLEMENTARIA

- Miranda Vargas, Horacio; Víctor González Escobar, Ruby Morales (septiembre 2016). Comunicación efectiva en ambientes digitales y su implicancia en la educación superior. https://www.academia.edu/2018426/COMUNICACI%C3%93N_EFECTIVA_EN_AMBIENTES_DIGITALES%20%E2%80%A2_Y_SU_IMPLICANCIA_EN_LA_EDUCACI%C3%93N_SUPERIOR
- Barrios, V. (2017) Política Nacional de Ciberseguridad, (2017-2022). Gobierno de Chile. https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/26760/1/POLITICA_NACIONAL_DE_CIBER.pdf